103 – Image Analysis

Team Information

Team Name: AWGN

Results Email: [redacted]

Examination Time Frame: 10/1 to 10/25/08

Instructions

Description: Examine the images in the **103_Image_Analysis_Challenge2008** folder. Provide evidence as to the metadata contained or recovered for each of the files. Note not only the metadata, but why it may be of investigative interest.

Points will be awarded for the recovered metadata, the notation of metadata of possible investigative interest, and reasoning for your decision.

Total Weighted Points: 5 Total Points available per file – Total 100 Points Available

1. **Answers** – Supply the found/recovered metadata.
2. **Investigative Interest** – Supply the information that you feel is of investigative interest and why you consider it as such.
3. **Methodology** – Provide details to support your decision.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

Report of Examination

Challenge Number: 103 - Image Analysis

Examiner: James Willmont JMW

Keyboard.jpg - Real unaltered image
Canon Canon powershot G7 was located at 0X904 while looking at the Keyboard.jpg file in notepad++, which imples that the image is a real photo and not CG. The metadata says the image was taken at a lens apperature of F/2.8 which would be consistent with the depth of field of the image. The apperature setting could have caused the image to have out of focus areas. Additionally, used Error Level Analysis in two ways. Used Error Level Analyzer from http://www.tinyappz.com/wiki/Error_Level_Analyser on the file to produce a heat map, but nothing conclusive was seen in terms of image manipulation. There is a suspicious spot in the middle of the image, see keboardheatmap.png but it appears that occurs from light on the subject. Additionally, used a custom python script to perform varying ELA at intervals of 15%.

beach_foot.jpg real altered image
0xB0 Canon Canon Powershot SD550 implies the image is a real photo.
0xDC Adobe Photoshop CS3 Windows 2008 implies the image was saved in photoshop and potentially altered, lots of other references to photoshop and the camera in the metadata.
See "beach_foot heatmap.png". Appears from the line on the leg that the leg was inserted in the image or altered in some way. Additionally, the heatmap image shows an unusual area at the top of the image of circular object that cannot be explained easily and which seems almost too perfect to appear in nature. Lastly in the heatmap where the shadow from the leg has an anomally as well. This area contains black while the rest of the image has only shades of blue.

bearded_guy.jpg Fake image/ composite
0x18 The word "Ducky" is present...(the web says the word ducky comes from images created by Adobe photoshop)
0x2B "Adobe" present leads to believe the image was at least edited with photoshop, however, this image doesn't have the abundance of metadata as the other images do.
The heatmap shows distinct lines around the head and the signature in red.
When zooming in, the edge of the head has a very jagged edge, but on the transition to the shoulder, the shoulder line becomes very smooth.

blue_eyes.jpg fake digital image
0x104F "photoshop" and Creation Software under properties says Adobe Photoshop CS3 Windows
The Heatmap shows distinct perfectly straight lines and areas that do not occur in nature, which implies that this is at least altered.

board.jpg real unaltered image
this appears to be a real image taken on 5/1/2003 at 10:14AM using a Casio EX-Z3. No mention of photoshop.

bride.jpg composite image
metadata: creation software = Adobe photoshop CS3 Windows
It appears the necklace at the very least was added to the image as visible edges can be seen.
It looks like certain parts of the image are not at the same quality of the rest of the image as can be in some of the ELA tests, in particular the neclace and hair.

brunette.jpg
Canon Powershot A620 on 11/23/2005 at 4.34pm. no photoshop mentioned. It appears to be a real image but could use some color adjustment as the image is very red.

curtain_lady.jpg composite image
creation software= Adobe Photoshop CS3 Windows
It appears she was added to the picture as the image has a sort of halo around her. Looks like a touch up rather than full CG. Additionally, by looking at the ELA images it appears that the the lady and the background image are at different levels.

eagle.jpg
canon EOS 350D Digital Camera. No mention of photoshop.
the ELA analysis is fairly inconclusive on this image as the body of the bird matches that of the sky, but the edges somewhat glow. The information from the camera seems accurate for the depth of field and lack of blur from motion.

elder_lady.jpg Fake altered image
This is definitely an altered image. I searched for the artist and found Marek Denko and his picture Clochard. The original doesn't have the black smudges around the picture. Additionally, the rest of Marek Denko's artwork is all 3-d images so it can be assumed that this image (which looks like a diarama almost) is a created image and not a real one.

girl.jpg.jpg Fake Image
metadata: creation software Adobe Photoshop CS3
First off, the face seems too elongated and almost plastic looking. When doing the ELA, the image has some blocky areas that don't seem man made.

girl_with_glasses.jpg Fake image
No metadata info in this image, but the eyes don't seem correct. It seems like they aren't connected, almost floating. Additionally, the ear is out of focus but the hair is.

guy.jpg real altered image
everything in this image seems like it is a real image, but when looking at the eyes something doesn't seem quite right. He has a large glare from a bright light on his face and jacket, yet his eyes don't have any light reflected off them. A glare falls on his upper eyelid, which could account for it.

lady_in_tshirt.jpg.jpeg
composite image
In the ELA images the head has a halo around it, but the tshirt does not. Leads me believe this is two separate images.

Leonardo.jpg
real digitally enhanced image
The picture has a few section on the heatmap that black when the rest of the image is shades of blue. The ELA doesn't reveal anything conclusive.

Sequin_girl.jpg composite image
The girl in the picture has disproportionately large eyes when compared to the rest of her features, which makes us believe it is a doll. the image has been manipualeted by inserting a black border around the image with almost a bevel. This can be seen in the heatmap image really well as a red line around the image. The red line surrounding the picture is not the only suspect area of the image. In fact, all of the clothes are of the same red color. This is echoed as well in the ELA images, to include the eyes and mouth.

tulips.jpg
metadata shows the camera to be real and shot by a Canon PowerShot A520. The heatmap and ELA do not reveal anything that leads us to believe this image has been tampered with.

veiled_lady.jpg real image that has been digitally enhanced
the ELA and heatmap show an area in the upper right hand corner that is composed of blocks (most easily seen in the heatmap image).

Methodology / Notes Form

Challenge Number: 103 - Image Analysis

Tool Information

Type	Name	Publisher
○ Commercial ◉ Open Source	Notepad++	notepad-plus.sourceforge.net
◉ Commercial ○ Open Source	Google Picasa	Google
○ Commercial ◉ Open Source	Error Level Analyzer	www.tinyappz.com/wiki/Error_Level_Analyzer
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		

Notes

Two techniques were used for obtaining the Metadata out of the files.

The first is Microsoft's right-click properties command. This shows nearly all the metadata that out other technique finds. In some operating systems it required the tab "advanced" to show the metadata.
The findings do not display all the metadata as it requires manual typing of the data. In some cases the metadata was camera model, creation software, shutter speed, aperture, etc. Others didn't display as much information if any.

The second method was using a hex editor, in our case we used
Notepad++ with the hex editor module from
http://notepad-plus.sourceforge.net/uk/download.php. By putting the information in hex some human readable translation is put to the side.
Additionally, by searching through the hex for the jpeg codes 0xFFF8 and 0XFFFA. This signifies the area where the metadata will reside as between these codes are the actual image data. In at least one instance this method found data that the Microsoft method did not.
The word Adobe and Ducky were both found in the image and a quick Google search revealed Ducky to be related to files created in Adobe Photoshop.